Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/diin

Digital Investigation

The growing impact of full disk encryption on digital forensics

Eoghan Casey [a,*], Geoff Fellows [b], Matthew Geiger [c], Gerasimos Stellatos [d]

[a] cmdLabs, 1101 E. 33rd Street, Suite C301, Baltimore, MD 21218, United States
[b] LG Training Partnership, United Kingdom
[c] CERT, United States
[d] CACI International, United States

ARTICLE INFO

Article history:
Received 16 March 2011
Received in revised form
17 September 2011
Accepted 24 September 2011

Keywords:
Digital forensics
Full disk encryption
Hard drive encryption
Volatile data
Memory forensics

ABSTRACT

The increasing use of full disk encryption (FDE) can significantly hamper digital investigations, potentially preventing access to all digital evidence in a case. The practice of shutting down an evidential computer is not an acceptable technique when dealing with FDE or even volume encryption because it may result in all data on the device being rendered inaccessible for forensic examination. To address this challenge, there is a pressing need for more effective on-scene capabilities to detect and preserve encryption prior to pulling the plug. In addition, to give digital investigators the best chance of obtaining decrypted data in the field, prosecutors need to prepare search warrants with FDE in mind. This paper describes how FDE has hampered past investigations, and how circumventing FDE has benefited certain cases. This paper goes on to provide guidance for gathering items at the crime scene that may be useful for accessing encrypted data, and for performing on-scene forensic acquisitions of live computer systems. These measures increase the chances of acquiring digital evidence in an unencrypted state or capturing an encryption key or passphrase. Some implications for drafting and executing search warrants to dealing with FDE are discussed.

1. Introduction

When digital investigators encounter encryption, it is often at the file system level and, even when it is not possible to recover any of the encrypted data, it may be possible to recover incriminating digital evidence from unencrypted areas of storage media sufficient to support prosecution. However, as full disk encryption (FDE) becomes more widely used, it may not be possible to recover any digital evidence in some cases. An earlier FDE paper presented a rather one-sided view of what to do when the FDE key/passphrase is available, but did not emphasize the negative impact that successful FDE can have on a digital investigation (Casey and Stellatos, 2008). This follow on paper is intended as a wakeup call to those who believe that FDE does not pose a problem from a forensic perspective.

There are a number of ways that FDE has hampered digital investigations. The first potential problem arises when there is a failure to recognize that FDE is in use on an evidential hard drive. When contraband is observed on a computer system that is running but digital investigators turn off the computer to preserve the digital evidence, FDE may prevent further access to the incriminating data. Alternately, when a hard drive is received by a digital forensic laboratory, it may not be part of the standard operating process to perform a forensic preview of stored media prior to acquiring a forensic duplicate. This omission can lead to a failure to recognize that FDE is present, resulting in wasted resources spent processing

* Corresponding author.
E-mail address: eoghan@disclosedigital.com (E. Casey).
1742-2876/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.diin.2011.09.005

encrypted data and lost investigative opportunities. Another potential problem arises when digital investigators fail to collect potential FDE passphrases or recovery keys at a crime scene. Such information may exist in written form or digital form on a recovery disk or in memory, potentially requiring digital investigators to acquire volatile data from computers at the scene. A more serious problem arises when a Trusted Platform Module (TPM) is involved and hardware alterations render encrypted digital evidence unrecoverable. In this situation, the damage may be irreversible and digital evidence may be unrecoverable even after an otherwise viable decryption mechanism becomes available.

Challenges can also arise when a defendant appears to be cooperative. For instance, the defendant may provide incorrect decryption details but the defense may claim that the encrypted container was damaged in some manner, which was why it would not open. In addition, encryption products such as TrueCrypt enable users to create two separate storage areas within an encrypted container, each with their own passphrases. Using this approach, a defendant could provide just one of the passphrases and digital investigators may not realize that additional evidence is concealed on the storage media.

With current resources, law enforcement's hands are tied when it comes to FDE when used by anyone who is diligent with the passphrase. In a growing number of cases it may be difficult to prosecute for a meaningful conviction because of the inability to access evidence on either FDE systems or in encrypted containers. In one case, a convicted computer criminal was found to be using computers, which was a violation of his probation. All of his computers were protected using TrueCrypt and he was never compelled to give up his passphrases by the court. Digital investigators tried everything in their immediate power to crack the encryption but to no avail. Digital investigators still do not know what was on the computers but suspect that the offender was involved in various criminal activities.

One desired outcome of this paper is to provide guidance for gathering items at the crime scene that may be useful for accessing encrypted data, and for performing on-scene forensic acquisitions of live computer systems prior to transporting the evidence to digital forensic laboratories. These measures increase the chances of acquiring digital evidence in an unencrypted state or capturing an encryption key or passphrase. Some implications for drafting and executing search warrants to deal with FDE are discussed. Finally, it is also our hope that this paper will motivate the development of new techniques to overcome FDE.

2. Increasing use of FDE

Until recently, offenders who use encryption rarely protected every piece of media in their entirety, and generally left some incriminating digital evidence in unencrypted form. As a result, digital investigators may have been able to recover sufficient evidence to support a prosecution but this is not always the case, particularly when FDE is involved.

There are a growing number of FDE products, and hard drive manufacturers are building FDE into storage media. Full disk or volume encryption products include open source (TrueCrypt), third party (McAfee's Safeboot, WinMagic's SecureDoc, Symantec's PGP and GuardianEdge), or integration within the native operating system itself. Although many of these products can be configured with an additional decryption key (ADK) that an organization can use to recover data, these options may not be employed by an individual who is using encryption to conceal criminal activities.

As an example, Microsoft Windows BitLocker Drive Encryption is available in the Enterprise and Ultimate editions of Windows Vista and Windows 7, and Windows Server 2008 (Microsoft, 2009, 2010). The implementation of BitLocker drive encryption requires a user to either initialize the TPM chip or configure authentication without a TPM via a USB flash drive. The TPM provides validation for the boot process, detection of hardware tampering, and storage of the Bitlocker master key. Authentication without a TPM requires a user to save the master key to a USB flash drive that must be connected to the device upon startup. Self-encrypting hard drives are being manufactured to meet the Opal standard established by the Trusted Computing Group in 2009. Fig. 1 shows the authentication screen for such an Opal-compliant self-encrypting hard drive. Any attempt to acquire data from such encrypted hard drives without the associated decryption passphrase will fail.

The growth of FDE solutions is not just limited to hard drives. Offenders can encrypt volumes on removable media natively with BitLocker, with open source tools such as TrueCrypt, or with tools purchased from vendors such as IronKey and SanDisk. The availability of encryption solutions and ease of implementation on hard drives and removable media have provided offenders with protection that cannot be circumvented if implemented correctly.

3. Investigations foiled by encryption

When encryption cannot be circumvented, it may not be possible to convict an offender of a crime. The following recent case examples are summarized to demonstrate the impact of encryption on an investigation.

Case Example: In the case of Brazilian banker Daniel Dantas, we see how a strong TrueCrypt passphrase has prevented access to encrypted data on hard drives seized from Dantas's apartment by the Brazilian police (Leyden, 2010). To date, neither dictionary-based attacks by the Brazilian National Institute of Criminology (INC) nor attempts by the FBI have succeeded in accessing the encrypted data.

In the United States, the Fifth Amendment protects defendants against self-incrimination, including disclosure of encryption keys in some cases.

Case Example: Customs officials observed potential child pornography on Sebastien Boucher's computer as he was crossing the Canadian border. However, his computer was turned off before a forensic duplicate was acquired, and all of the alleged child pornography was inaccessible apparently because it was locked in an encrypted volume. When

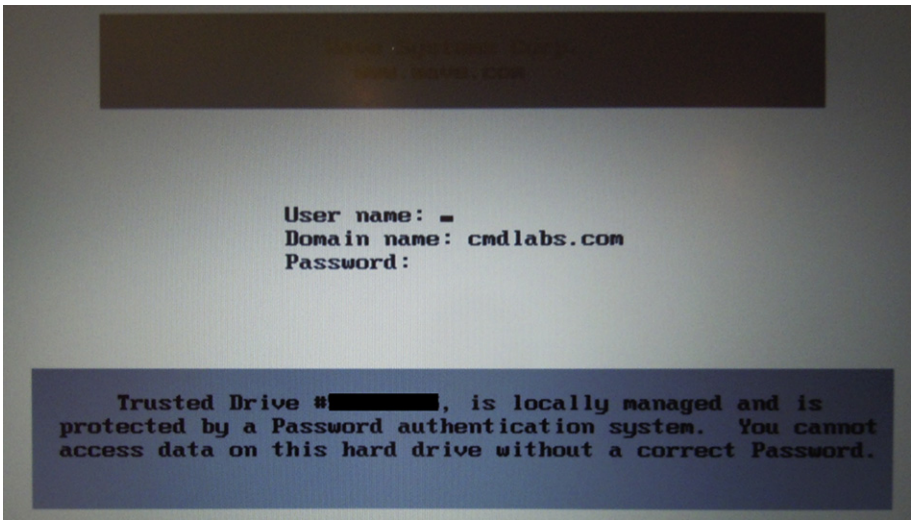

Fig. 1 – Authentication screen for Opal-compliant self-encrypting hard drive.

prosecutors attempted to compel Boucher to unlock the encrypted data he pled the Fifth, preventing recovery of the encrypted data.

In the UK, legislation allows for a maximum of 5 years in prison for terrorist suspects that do not provide encryption passphrases when required by law. In the context of cases other than terrorist cases, the maximum sentence is 2 years.

Case Example: A suspected terrorist was apprehended with his laptop open and turned on with the TrueCrypt Mount window displayed on screen. Part of the passphrase for a 1 GB TrueCrypt volume had been typed into the TrueCrypt Mount window. The screen contents and partial passphrase were noted by the police before the laptop was seized, imaged and examined. The suspect was asked in interview for the full passphrase but he refused until an order was obtained from the High Court requiring him to disclose the passphrase. However, the passphrase he provided did not work. In court, the suspect stated that he believed that that was the correct passphrase, but it was months since he had even seen his computer and he may not be remembering correctly. Based on this situation, the judge held that there was no case to answer.

These few cases demonstrate the serious challenge that FDE poses for digital forensics.

4. Investigations bolstered by overcoming encryption

In some cases, there may be enough digital evidence to bring some charge but the recovery of encrypted data may make a dramatic difference in the charges brought and in the scope of crimes resolved. Several recent high-profile cases demonstrate the impact that overcoming encryption can have on an investigation. It is worth noting that searches and evidence acquisition in these cases were specifically planned to address, as far as possible, the obstacles presented by FDE and encrypted containers.

Case Example: Albert Gonzalez and his associates, convicted in 2009 for a string of intrusions including TJX Corp and Heartland Payment Systems, widely employed FDE and encrypted containers. Because of the expectation that encrypted storage was prevalent, the pre-raid preparations and on-scene search strategies were crafted to maximize the opportunity to gain access to running systems and the data they contained. As a result of this careful planning and the ability to gain access to an FDE system at one of the first crime scenes that digital investigators processed during a coordinated series of searches led by the US Secret Service, critical information was exposed that paved the way for the recovery of a much larger trove of evidence – and eventually to successful prosecution of the organization.

Case Example: As part of the recent situation involving a US-based Russian spy ring, the Federal Bureau of Investigation (FBI) successfully circumvented full disk encryption utilized by the Russian agents. The FBI was able to access and analyze their acquired forensic images of the encrypted devices because during their searches they recovered pieces of paper containing the necessary passphrases. It begs the questions of what would have happened had the Russian agents not written them down (U.S. v. Anna Chapman and Mikhail Semenko).

Case Example: In the Max Ray Butler (Iceman) case, the digital investigators expected to encounter encryption and the on-scene search was planned accordingly to maximize the opportunity to gain access to running systems, whether they were locked or not. Gaining access to cryptographic data during the search permitted the subsequent decryption of his FDE systems and an assortment of encrypted containers on external drives. This greatly added to initial evidence of the sale of encoding data for several thousand credit cards, leading to Butler's eventual

conviction for the theft of data for nearly 2 million unique payment cards. It also gave investigators access to artifacts from more than a hundred intrusions over several years.

These cases demonstrate the value of preparing for FDE from the perspective of prosecutors, investigators and forensic practitioners.

5. Approaches to tackling full disk encryption

In the era of FDE, pulling the plug from a computer is not an acceptable response technique when encountering FDE or even volume encryption. Although it is a good practice to document written passphases and to collect removable media that may contain recovery keys, additional approaches are needed to increase the chances that encrypted data will be preserved. Digital investigators must increase their capabilities to detect encryption in the field prior to pulling the plug. Moreover, the ability to develop and implement live acquisition techniques is essential, as the use of FDE continues to grow.

While processing a crime scene, digital investigators can preserve volatile and non-volatile data from a "live" system that is utilizing FDE or that has mounted encrypted containers. Because these encryption implementations are decrypted on the fly on running systems, live imaging of the non-volatile data will give access to content that would otherwise be encrypted on a "dead" system. In addition, data recovered from volatile memory may provide access to encrypted content on the device. Fig. 2 shows a passphrase "accountdata" that was cached in memory by TrueCrypt and was captured and recovered using forensic tools.

The preservation of volatile memory for many versions of Windows operating systems can be accomplished through the use of acquisition tools such as MoonSols Windows Memory Toolkit (http://www.moonsols.com), GMG Systems's KnTTools (http://gmgsystemsinc.com) and HBGary's Fastdump Pro (http://www.hbgary.com) as shown in Fig. 3.

Other methods of acquiring physical memory dumps are available, including Firewire direct memory access tools such as Passware Kit Forensic (http://www.lostpassword.com/kit-forensic.htm) and remote forensic tools such as F-Response (http://www.f-response.com). Once acquired, physical memory dumps can be examined using specialized tools such as Volatility (http://www.volatilesystems.com/), MoonSols Windows Memory Toolkit, HBGary's Responder, Mandiant's Memoryze (www.mandiant.com) and KnTList from GMG Systems.

Live acquisition of non-volatile data on a computer using FDE can be preserved with the use of a portable imaging tool such as AccessData's FTK Imager as shown in Fig. 4. The screen in the background shows an encrypted TrueCrypt volume mounted as drive letter "T:" and the screen in the foreground shows a forensic duplicate of this decrypted volume being acquired using FTK Imager Lite.

Of course, all this presupposes gaining interactive access to running computer systems, which usually requires extra measures on the part of investigators, participating attorneys and the search team. In a law enforcement setting, maximizing the likelihood of recovering evidence as FDE and encrypted containers become pervasive means adapting the legal, tactical and technical frameworks for search and seizure.

5.1. *Adapting the legal approach*

Clearly articulating the risk to the preservation of evidence posed by encryption helps prosecutors secure search conditions that boost the chances of success. These favorable conditions include search warrants that permit surprise entry, so-called "No-knock" warrants, and warrants that can be

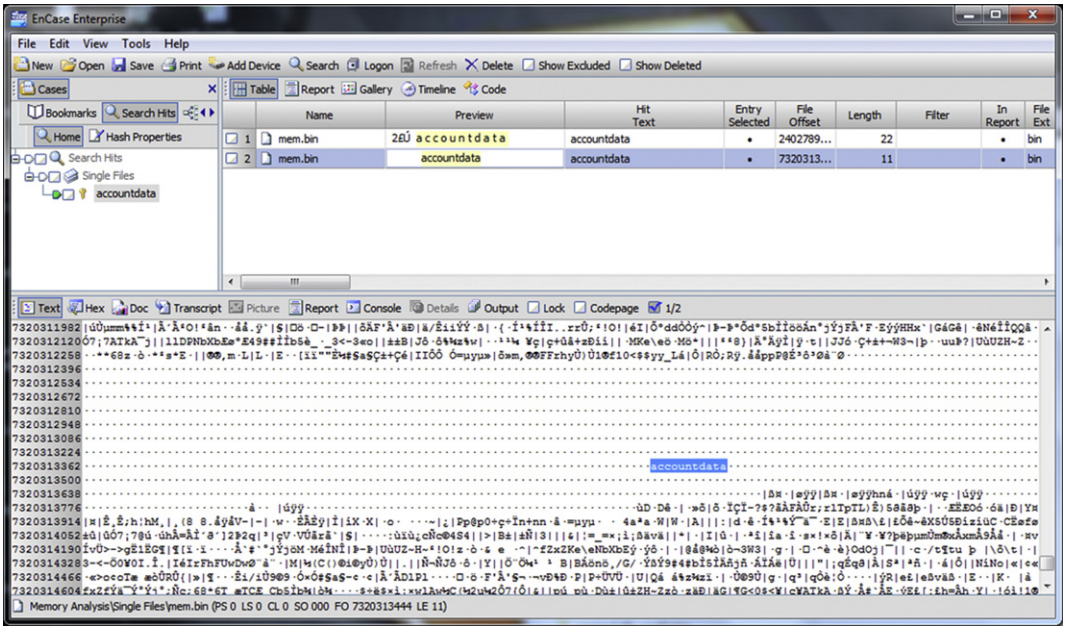

Fig. 2 – Example of encryption passphrase found in physical memory dump.

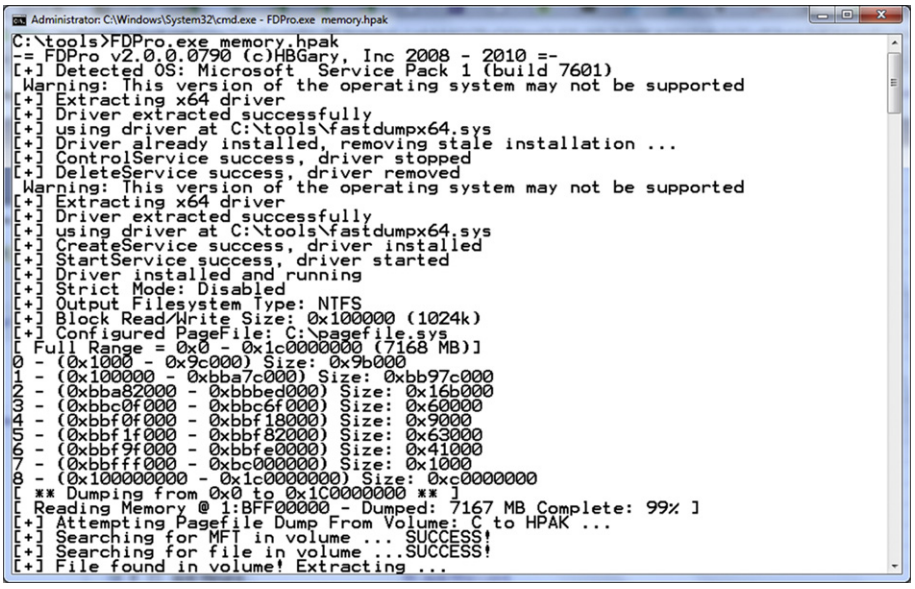

Fig. 3 – HBGary Fastdump Pro running on a live computer to acquire physical memory and pagefile.

executed in the middle of the night. Precedent exists for such warrants in computer crime cases, but prosecutors and investigators need to lay the groundwork to secure the judge's approval for them.

In addition, there are cases where the only practical path to ensure the recovery of passphrases or keys for encrypted devices involves gaining access to the search site or target system to install software or hardware devices that intercept and record the keys. Warrants of this type, known as delayed notification (or Sneak-and-Peek) warrants, are reasonably rare outside of national security cases and usually require considerable work to obtain approval.

Gaining access to encrypted systems frequently involves a higher level of interaction by the practitioner collecting the data. Indeed, the "interaction" may include actually breaking into the computer system. So, prosecutors would be wise to anticipate legal challenges that stem from allegations that this renders less reliable the evidence obtained in this fashion.

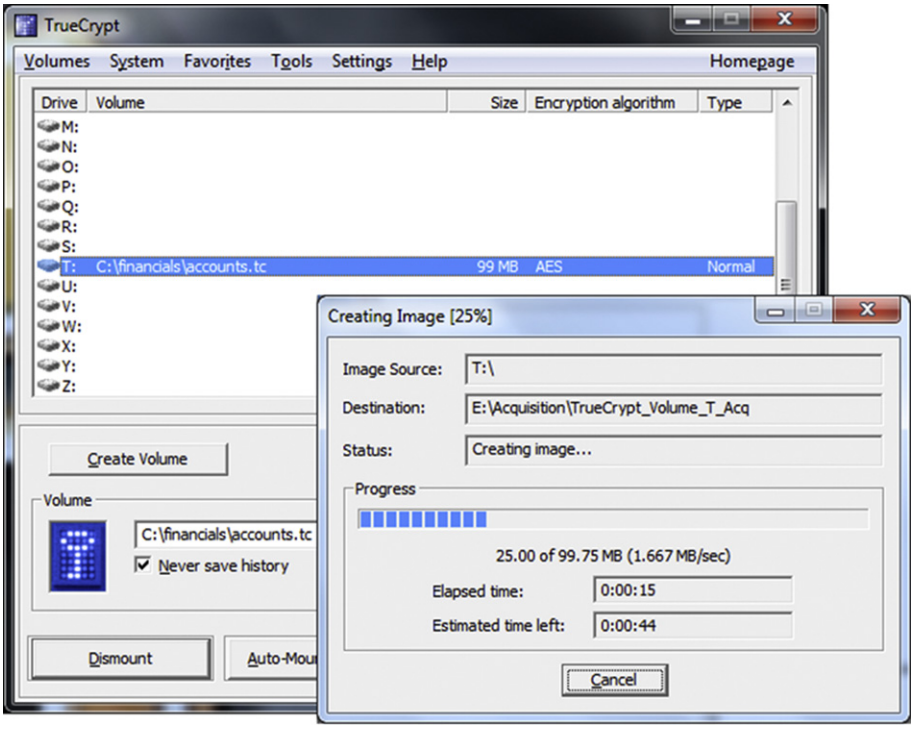

Fig. 4 – FTK Imager Lite running on a live computer to acquire an encrypted volume.

Advance planning of legal responses and procedures that mitigate this challenge may well be less cumbersome than setting bad precedent in this arena.

5.2. *Adapting the tactical approach*

From the point of view of investigators, coping with encryption places an emphasis on intelligence gathering on that topic in advance of planning a search or evidence collection. If the goal is to gain access to running systems, important intelligence will typically include details such as when the targets conduct their activity, the physical layout of the search site, any early warning systems or countermeasures (in addition to encryption), the operating systems, hardware configuration and types of encryption used. This information is used to develop a plan with the search team that will maximize surprise and reduce the opportunity for anyone to power off or damage a system. At the same time, the initial search team should designate members who will identify and preserve any access to running systems, even simply generating mouse movements to prevent account access from timing out.

5.3. *Adapting acquisition procedures*

As pervasive as the use of encryption has become, there is seldom a good reason for on-scene digital investigators not to screen running systems for active encryption. Similarly, obtaining live forensic duplicates of decrypted storage media and acquiring physical memory from running systems has become a sensible routine procedure if doubt about the use of encryption exists.

Depending on the circumstances, it may be advisable to gain access to a running system while it is still in-situ, starting with a minimal interaction approach. On an unlocked Windows computer, digital investigators may be able to determine that FDE is present by simply review the System tray and Program Files folder, or by reviewing logical drives and their file system type. To assist with basic screening in this regard, CERT at Carnegie Mellon University developed a law-enforcement-restricted utility called CryptHunter that alerts to FDE and mounted encrypted containers on a running system (https://www.cert.org/forensics/). The purpose of this tool is precisely to flag these more complex acquisition scenarios to on-scene responders, who may then request additional guidance and resources, if necessary.

When a password protected computer is encountered, it may be possible to circumvent the security mechanism and acquire data from the computer using specialized tools. For instance, the Passware Kit Forensic implements a direct memory access (DMA) approach via Firewire that can acquire memory from some locked computer systems. Alternately, if there are accessible devices on a local network these may have trusted status that can be used to escalate access on the target system.

Another adaptation is the capability to collect and transport running systems that are believed to employ encryption, but that offer no interactive access because an account is locked or none are logged in. Tools such as the HotPlug by Wiebetech allow technicians to transfer a running system to a backup power source for transportation. This will give practitioners and specialists the opportunity to review possible mechanisms to gain access to the system, such as exploiting a vulnerability in a running service.

6. Conclusions

The increasing use of full disk encryption has far reaching implications in digital forensics. Digital investigators must be prepared to confront FDE at the crime scene and prosecutors need to prepare search warrants with FDE in mind. On-scene protocols need to be adapted to obtain the information necessary to tackle FDE. Digital forensic laboratories need to update standard operating procedures to ensure that encrypted disks and volatile data are processed efficiently and effectively to bolster the chances of recovering encrypted data from computer systems. Finally, research is needed to develop new techniques and technology for breaking or bypassing full disk encryption. Without these measures in place, FDE will increasingly hamper digital investigations.

REFERENCES

Casey E, Stellatos G. The impact of full disk encryption on digital forensics. ACM SIGOPS Operating Systems Review April 2008; 42(3).

Leyden J. Brazilian banker's crypto baffles FBI: 18 months of failure. The Register. Available online at, http://www.theregister.co.uk/2010/06/28/brazil_banker_crypto_lock_out/; June 28 2010.

Microsoft. BitLocker Drive Encryption step-by-step guide. Microsoft Technet, http://technet.microsoft.com/en-us/library/cc732725(WS.10).aspx; November 3 2009.

Microsoft. BitLocker Drive Encryption overview. Microsoft Website, http://windows.microsoft.com/en-US/windows-vista/BitLocker-Drive-Encryption-Overview; 2011.

U.S. v. Anna Chapman and Mikhail Semenko, Southern District of New York (Available online http://documents.nytimes.com/criminal-complaints-from-the-justice-department).